Global Information Assurance Certification Paper

DNS Remote Root Exploit - ADM Named 8.2/8.2.1 NXT Remote Overflow

Ken Athanasiou

April 17, 2000

This exploit uses a buffer overflow in BIND (Short for ***B**erkeley **I**nternet **N**ame **D**omain,* a Domain Name Server (DNS). BIND is designed for Unix systems based on BSD, the version of Unix developed at the University of California's Berkeley campus) versions 8.2 – 8.2.2 to gain a remote shell with root authority. It uses DNS port 53 on the local machine and acts as a valid DNS server waiting for queries. When another DNS server queries the attacker machine it will send an invalid NXT response that will cause a buffer overflow and contains code to grant you remote root to any vulnerable BIND server. You can get the exploit from http://www.hack.co.za/exploits/daemon/named/t666.c

The applicable CERT advisory is listed below. Only the vulnerability specific to this exploit is listed out of the six BIND vulnerabilities covered in the advisory.

CERT® Advisory CA-99-14 Multiple Vulnerabilities in BIND (original release date 10 Nov 1999)

Vulnerability #1: the "nxt bug"

> "Some versions of BIND fail to properly validate NXT records. This improper validation could allow an intruder to overflow a buffer and execute arbitrary code with the privileges of the name server.
>
> NXT record support was introduced in BIND version 8.2. Prior versions of BIND, including 4.x, are not vulnerable to this problem. The ISC-supplied version of BIND corrected this problem in version 8.2.2.
>
> By exploiting this vulnerability, remote intruders can execute arbitrary code with the privileges of the user running *named*, typically root. "

DNS Definition:

DNS stands for Domain Name Service which is an Internet service designed to translate easily remembered alphabetic names (mydomain.com) into what the Internet routers need which is IP addresses (198.168.23.124). The DNS system is based on it's own particular network of question and reply, i.e. if the queried DNS server doesn't know the translation for a particular domain name it asks another one until it can locate the right IP address. A DNS Server contains two zone files, one of which is used to lookup IP to hostname resolution and the other for hostname to IP resolution. This is vital for the exploit to function.

The most common method of directly querying a DNS server is through the use of nslookup (both in Unix based systems and Windows NT). This utility can be used to either resolve an IP to a domain name or vice versa simply by typing nslookup <IP> or nslookup <domain.name> as long as you have configured your TCP/IP service with a DNS server. The interactive mode of nslookup is more powerful and entered by simply typing nslookup. At the ">" prompt you can start entering IP addresses or hostnames to resolve which IP goes with what name and vice versa. There are also numerous commands that can allow you to get other information from nslookup. The various nslookup commands include set (for various options), server and lserver, finger, root, ls, and view. For an explanation of these options, check your man file.

To find a DNS server vulnerable to this exploit you can use DiG (available in most distributions (command format: dig @<server_ip> <domain> <query-type> <query-class>)). Once you identify a possibly accessible server (NMap scanning port 53) you can use a couple of ways to tell the version number BIND that is running, such as looking for the message that named puts in the syslog file on startup. Using nslookup: (with version 4.9.7 or higher)

```
# nslookup

Default Server: ns.yourco.bogus

Address: 333.333.333.333
```

> set class=chaos

> set type=txt

> version.bind

Server: ns.yourco.bogus

Address: 333.333.333.333

VERSION.BIND text = "8.2.2-P5"

>

The command 'ndc -t status' works on some systems and 'what < your-path-to > /named' works on some systems. The following commands will work if your version of BIND is 4.9.5 or greater:

dig version.bind txt chaos @ < server >

or

dig @ < server > txt chaos version.bind

If you see 8.2 or 8.2.1 or 8.2.2 then this server should be vulnerable. Anything else means it's not likely to work. According to the Internet Software Consortium BIND vulnerabilities page the vulnerable versions of the software are 8.2, 8.2 patch 1, and 8.2.1.

To set up this exploit you'll need root access to a primary DNS server on the Internet which is Authoritative for a domain on the net, an identified target box, and a machine from which to run it. For the DNS setup you'll need to get a sub-domain added to that DNS box you've got root on (you might be able to sweet talk a friend to get this done…). Just add a sub-domain NS record into the zone file that resolves to your machine's IP address and restart the name server service. To add the NS record you'll need to find the location of the zone file by looking in /etc/named.conf and look for something like 'directory "/var/named";' This is the directory the zone files will be in. Look in named.conf for a line that says 'type master;' the file line below that will tell you the name of the file you need to edit. It will look something like:

Zone "mydomain.com"{

Type master;

File "mydomain.com.zone"};

If you cat this file you'll see a SOA record at the top of the file and below it entries that look like:

@ IN NS NS.UU.mydomain.com.

You'll see there are A records which are hostname to IP record types, CNAME (Canonical Name) which are aliases to A records and NS records which are name server records that state what the name server is for a domain or sub-domain. PTR records, which relate IP addresses to fully qualified domain names, shouldn't exist in the zone file you want to edit. They exist in the second of the two zone files.

You want to make the name server for 'mysubdomain.mydomain.com' equal to the IP address of your 'attacking.box.com'. The format of the NS record you'll want to put in is this:

mysubdomain IN NS attacking.box.com.

Don't forget the trailing period. Restart the name server service with '/usr/sbin/ndc restart'.

Once you've gotten your NS record into the DNS server and restarted the service you need to get the exploit, patch it, compile it, and run it. The exploit does require a patch to make it work. ADM changed three characters so that when it runs the shell it looks for /adm/sh instead of /bin/sh. Search the source code for "/adm/" (0x2f,0x61,0x64,0x6d,0x2f) and replace it with "/bin/" (0x2f,0x62,0x69,0x6e,0x2f).

If you run the exploit without any switches it will return a list of the architectures it is designed to work on. You'll need to run the exploit for a specific architecture by using one of the switches. Once run it is bound to port 53 and listening for queries. Query the target for a host inside the sub-domain you added in the primary DNS server and the target will be directed to the appropriate IP address to look it up (the attacker box).

```
Nslookup
>server <target>
>www.mysubdomain.mydomain.com
```

The target server will query mydomain.com then mydomain.com will pass the IP address of attacker.box.com as the nameserver for mysubdomain.com and the target will query attacker.box.com. When the target DNS server queries the attacker box you'll see something like 'Received request from 198.168.198.168:2156 for subdomain.domain.com type=x'. If the DNS server querying the attacker box is vulnerable and you did everything else correctly you'll get a remote root shell.

This exploit will crash named on the target box so if you're running one of the vulnerable versions and notice an unexplained crash you may want to examine your logs for suspicious activity occurring directly after the crash. You should be running Tripwire or some other intrusion detection/configuration checking software on your system and exporting your system logs to another machine. That will allow you to identify if an attacker has installed a backdoor trojan or rootkit package on your DNS server. If you are interested in researching the available tools to detect the installation of a rootkit or are curious of the capabilities offered by rootkits go to http://packetstorm.securify.com/ and enter the search term "rootkit". You will get a nice listing of some available rootkits, scanners, and daemons to detect them.

The recommended solution to protect yourself from this exploit is to upgrade your BIND to the most recent version (currently 8.2.2 patch 5) as the versions below 8.2.2 patch level 2 all have serious vulnerabilities. You can get more information on BIND and other vulnerabilities associated with the software at http://www.isc.org/products/BIND/. There are no other work-arounds to solve this vulnerability without crippling the intended purpose of the software package.

Sources:

Horizon/Plaguez, ADM Crew, "ADM named 8.2/8.2.1 NXT remote overflow", http://www.hack.co.za/daem0n/named/t666.c, (9 Apr 2000)

Aleph One, "Smashing The Stack For Fun and Profit", Phrack Magazine (Vol VII, Issue 49), http://www.phrack.com/search.phtml?view&article=p49-14, (10 Apr 2000)

Unkown author, "DNS" and "BIND", http://www.webopedia.com, (10 Apr 2000)

CERT Advisory CA-99-14 Multiple Vulnerabilities in BIND, http://www.cert.org/advisories/CA-99-14-bind.html, (9 Apr 2000)

Internet Software Consortium, http://www.isc.org/products/BIND/bind-security-19991108.html, (11 Apr, 2000)

Securify Inc., Packetstorm, http://packetstorm.securify.com/, (9 Apr 2000)